



CVE-2022-23305

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2022-23305
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-18 16:15:00 UTC
Updated	2023-02-24 15:30:00 UTC
Description	By design, the JDBCAppender in Log4j 1.2.x accepts an SQL statement as a configuration parameter where the values to k

Risk And Classification

Problem Types: CWE-89

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Log4j	All	All	All	All
Application	Broadcom	Brocade Sannav	-	All	All	All
Application	Netapp	Snapmanager	-	All	All	All
Application	Netapp	Snapmanager	-	All	All	All
Application	Oracle	Advanced Supply Chain Planning	12.1	All	All	All
Application	Oracle	Advanced Supply Chain Planning	12.2	All	All	All
Application	Oracle	Business Intelligence	12.2.1.3.0	All	All	All
Application	Oracle	Business Intelligence	12.2.1.4.0	All	All	All
Application	Oracle	Business Intelligence	5.9.0.0.0	All	All	All
Application	Oracle	Business Process Management Suite	12.2.1.3.0	All	All	All
Application	Oracle	Business Process Management Suite	12.2.1.4.0	All	All	All
Application	Oracle	Communications Eagle Ftp Table Base Retrieval	4.5	All	All	All
Application	Oracle	Communications Instant Messaging Server	10.0.1.5.0	All	All	All
Application	Oracle	Communications Messaging Server	8.1	All	All	All
Application	Oracle	Communications Network Integrity	7.3.6	All	All	All
Application	Oracle	Communications Offline Mediation Controller	All	All	All	All
Application	Oracle	Communications Offline Mediation Controller	12.0.0.5.0	All	All	All

Application	Oracle	Communications Unified Inventory Management	7.4.1	All	All	All
Application	Oracle	Communications Unified Inventory Management	7.4.2	All	All	All
Application	Oracle	E-business Suite Cloud Manager And Cloud Backup Module	All	All	All	All
Application	Oracle	E-business Suite Cloud Manager And Cloud Backup Module	2.2.1.1.1	All	All	All
Application	Oracle	E-business Suite Information Discovery	All	All	All	All
Application	Oracle	Enterprise Manager Base Platform	13.4.0.0	All	All	All
Application	Oracle	Enterprise Manager Base Platform	13.5.0.0	All	All	All
Application	Oracle	Financial Services Revenue Management And Billing Analytics	2.7.0.0	All	All	All
Application	Oracle	Financial Services Revenue Management And Billing Analytics	2.7.0.1	All	All	All
Application	Oracle	Financial Services Revenue Management And Billing Analytics	2.8.0.0	All	All	All
Application	Oracle	Healthcare Foundation	8.1.0	All	All	All
Application	Oracle	Hyperion Data Relationship Management	All	All	All	All
Application	Oracle	Hyperion Infrastructure Technology	All	All	All	All
Application	Oracle	Identity Management Suite	12.2.1.3.0	All	All	All
Application	Oracle	Identity Management Suite	12.2.1.4.0	All	All	All
Application	Oracle	Identity Manager Connector	11.1.1.5.0	All	All	All
Application	Oracle	Jdeveloper	12.2.1.3.0	All	All	All
Application	Oracle	Middleware Common Libraries And Tools	12.2.1.4.0	All	All	All
Application	Oracle	Mysql Enterprise Monitor	All	All	All	All
Application	Oracle	Retail Extract Transform And Load	13.2.5	All	All	All
Application	Oracle	Tuxedo	12.2.2.0.0	All	All	All
Application	Oracle	Weblogic Server	12.2.1.3.0	All	All	All
Application	Oracle	Weblogic Server	12.2.1.4.0	All	All	All
Application	Oracle	Weblogic Server	14.1.1.0.0	All	All	All
Application	Qos	Reload4j	All	All	All	All

References

Reference	Source	Link	Tags
Oracle Critical Patch Update Advisory - April 2022	MISC	www.oracle.com	
oss-security - CVE-2022-23305: SQL injection in JDBC Appender in Apache Log4j V1	MLIST	www.openwall.com	
CVE-2022-23305 Apache Log4j Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
Apache log4j 1.2 -	MISC	logging.apache.org	
lists.apache.org/thread/pt6lh3pbsvxqjwlp4c5l798dv2hkc85y	MISC	lists.apache.org	
Oracle Critical Patch Update Advisory - July 2022	N/A	www.oracle.com	
CVE Program record	CVE.ORG	www.cve.org	canonical

Vendor Comments And Credit

Discovery Credit

LEGACY: Daniel Martin of NCC Group

Legacy QID Mappings

150538 Oracle WebLogic Server Multiple Vulnerabilities (CPUAPR2022)
159603 Oracle Enterprise Linux Security Update for parfait:0.5 (ELSA-2022-0290)
159628 Oracle Enterprise Linux Security Update for log4j (ELSA-2022-0442)
159853 Oracle Enterprise Linux Security Update for log4j (ELSA-2022-9419)
179047 Debian Security Update for apache-log4j1.2 (DLA 2905-1)
179238 Debian Security Update for apache-log4j1.2 (CVE-2022-23305)
199275 Ubuntu Security Notification for Apache Log4j Vulnerabilities (USN-5998-1)
240034 Red Hat Update for parfait:0.5 (RHSA-2022:0289)
240035 Red Hat Update for parfait:0.5 (RHSA-2022:0290)
240036 Red Hat Update for parfait:0.5 (RHSA-2022:0291)
240059 Red Hat Update for JBoss Enterprise Application Platform 7.4 (RHSA-2022:0436)
240060 Red Hat Update for JBoss Enterprise Application Platform 6.4 (RHSA-2022:0438)
240062 Red Hat Update for rh-maven36-log4j12 (RHSA-2022:0439)
240067 Red Hat Update for log4j (RHSA-2022:0442)
240078 Red Hat Update for red hat jboss web server 3.1 service pack 14 (RHSA-2022:0524)
240209 Red Hat Update for JBoss Enterprise Application Platform 7.4.4 (RHSA-2022:1296)
240210 Red Hat Update for JBoss Enterprise Application Platform 7.4.4 (RHSA-2022:1297)
240452 Red Hat Update for parfait:0.5 (RHSA-2022:0294)
240508 Red Hat Update for JBoss Enterprise Application Platform 6.4.2 (RHSA-2022:5459)
240511 Red Hat Update for JBoss Enterprise Application Platform 6.4.2 (RHSA-2022:5460)
257151 CentOS Security Update for log4j (CESA-2022:0442)
353173 Amazon Linux Security Advisory for log4j : ALAS2-2022-1750
354858 Amazon Linux Security Advisory for log4j : ALAS-2023-1718

355080 Amazon Linux Security Advisory for log4j : AL2012-2023-404
376438 IBM WebSphere Application Server Arbitrary Code Execution Vulnerability (Log4Shell) (6557248)
376639 IBM Integration Bus and IBM App Connect Enterprise Apache Log4j Vulnerabilities (6568731)
377086 Alibaba Cloud Linux Security Update for log4j (ALINUX2-SA-2022:0010)
377147 Alibaba Cloud Linux Security Update for parfait:0.5 (ALINUX3-SA-2022:0006)
377908 Oracle Coherence January 2023 Critical Patch Update (CPUJAN2023)
671400 EulerOS Security Update for log4j (EulerOS-SA-2022-1330)
671679 EulerOS Security Update for log4j (EulerOS-SA-2022-1744)
730542 Atlassian Confluence Server and Confluence Data Center Log4j Multiple Vulnerabilities (CONFSERVER-78991)
730566 Atlassian Jira Server and Data Center Log4j Vulnerability (JRASERVER-73885)
731338 Atlassian Bamboo Server and Data Center Multiple Security Vulnerabilities (BAM-21696, BAM-21697)
751667 SUSE Enterprise Linux Security Update for log4j (SUSE-SU-2022:0212-1)
751669 SUSE Enterprise Linux Security Update for log4j (SUSE-SU-2022:0214-1)
751670 OpenSUSE Security Update for log4j (openSUSE-SU-2022:0214-1)
751672 SUSE Enterprise Linux Security Update for log4j12 (SUSE-SU-2022:0226-1)
751673 OpenSUSE Security Update for log4j12 (openSUSE-SU-2022:0226-1)
753187 SUSE Enterprise Linux Security Update for log4j (SUSE-SU-2022:14881-1)
87489 Oracle WebLogic Server Multiple Vulnerabilities (CPUAPR2022)
940440 AlmaLinux Security Update for parfait:0.5 (ALSA-2022:0290)
960689 Rocky Linux Security Update for parfait:0.5 (RLSA-2022:0290)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)